ABSTRACT OF THE DISCLOSURE

A security key, such as an encryption key, is generated so as to make it more difficult for eavesdroppers to identify the key. Specifically, a cryptographically secure random number generator generates a random bit sequence that is included in a seed. This random seed is provided along with a negotiated master secret to a key generation module. The key generation module may implement a pseudo random function that is in accordance with the Transport Layer Security (TLS) protocol or the Wireless Transport Layer Security (WTLS) protocol. This key may then be used to encrypt a plain text message to form an encrypted data packet. The encrypted data packet also includes the random seed in unencrypted form. The encrypted data packet may be transmitted over a public network to a recipient with reduced risk of eavesdropping.

G:\DATA\PAT\WORDPAT\13768.191.doc